

FIG. 1

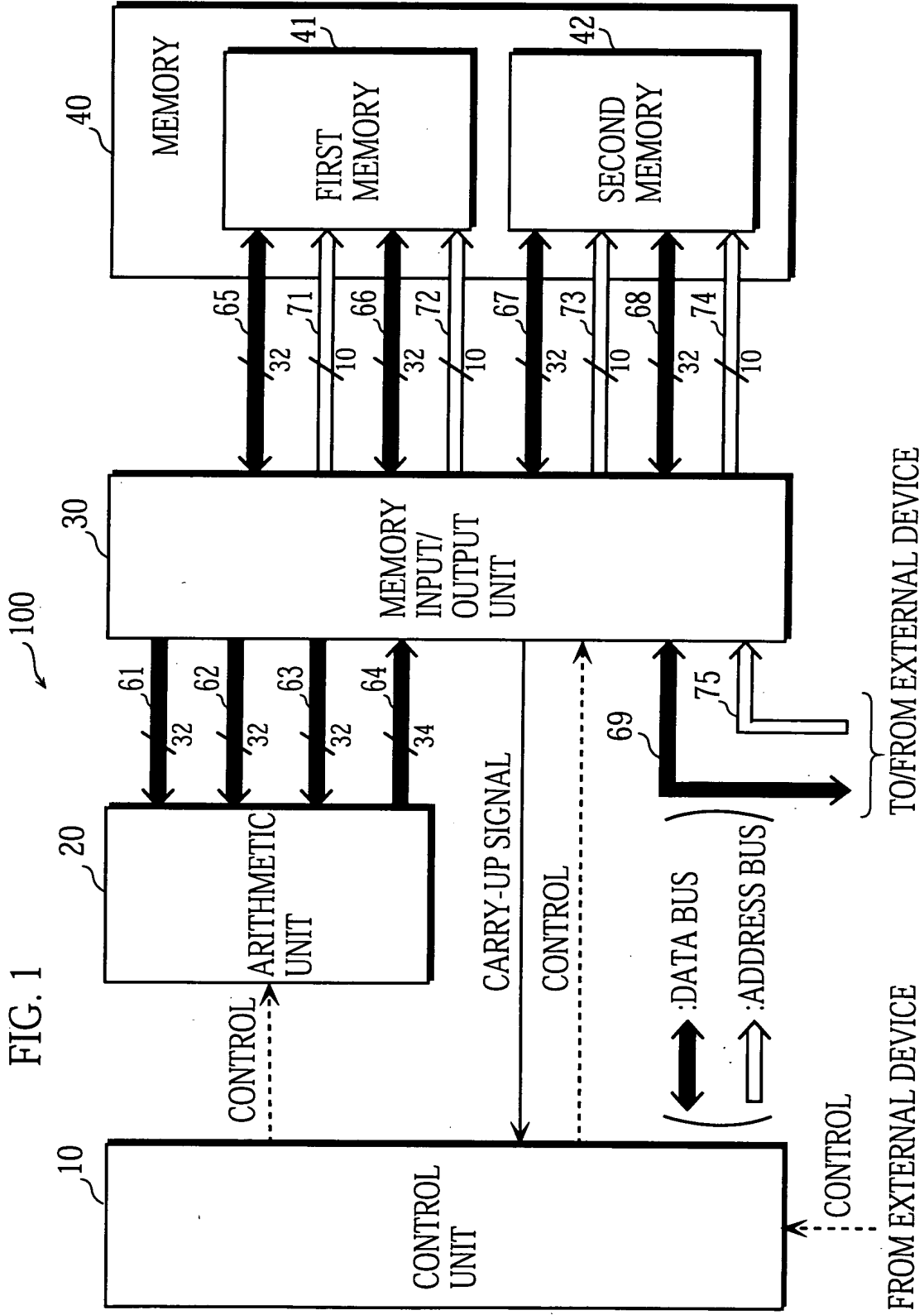


FIG. 2

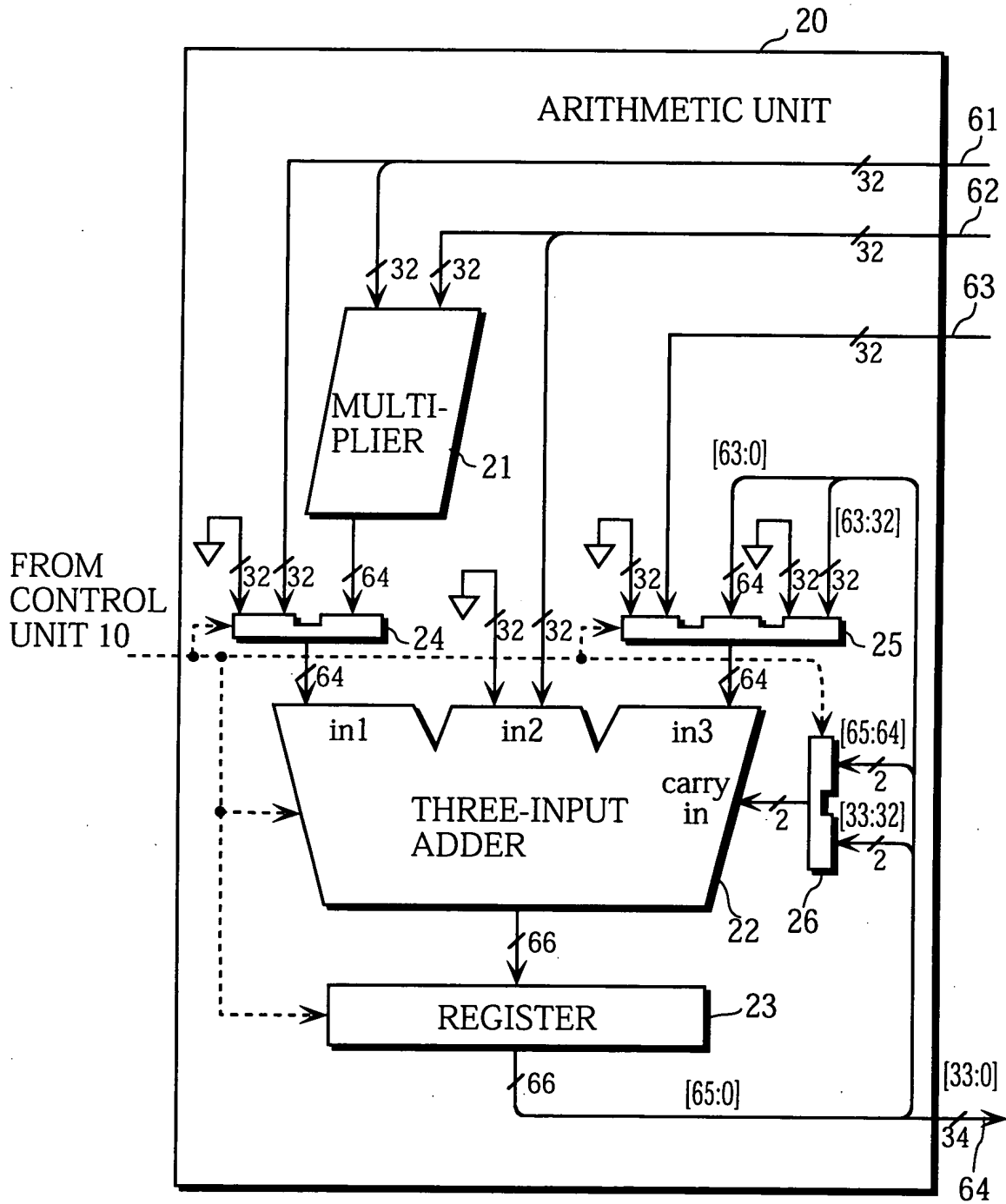


FIG. 3

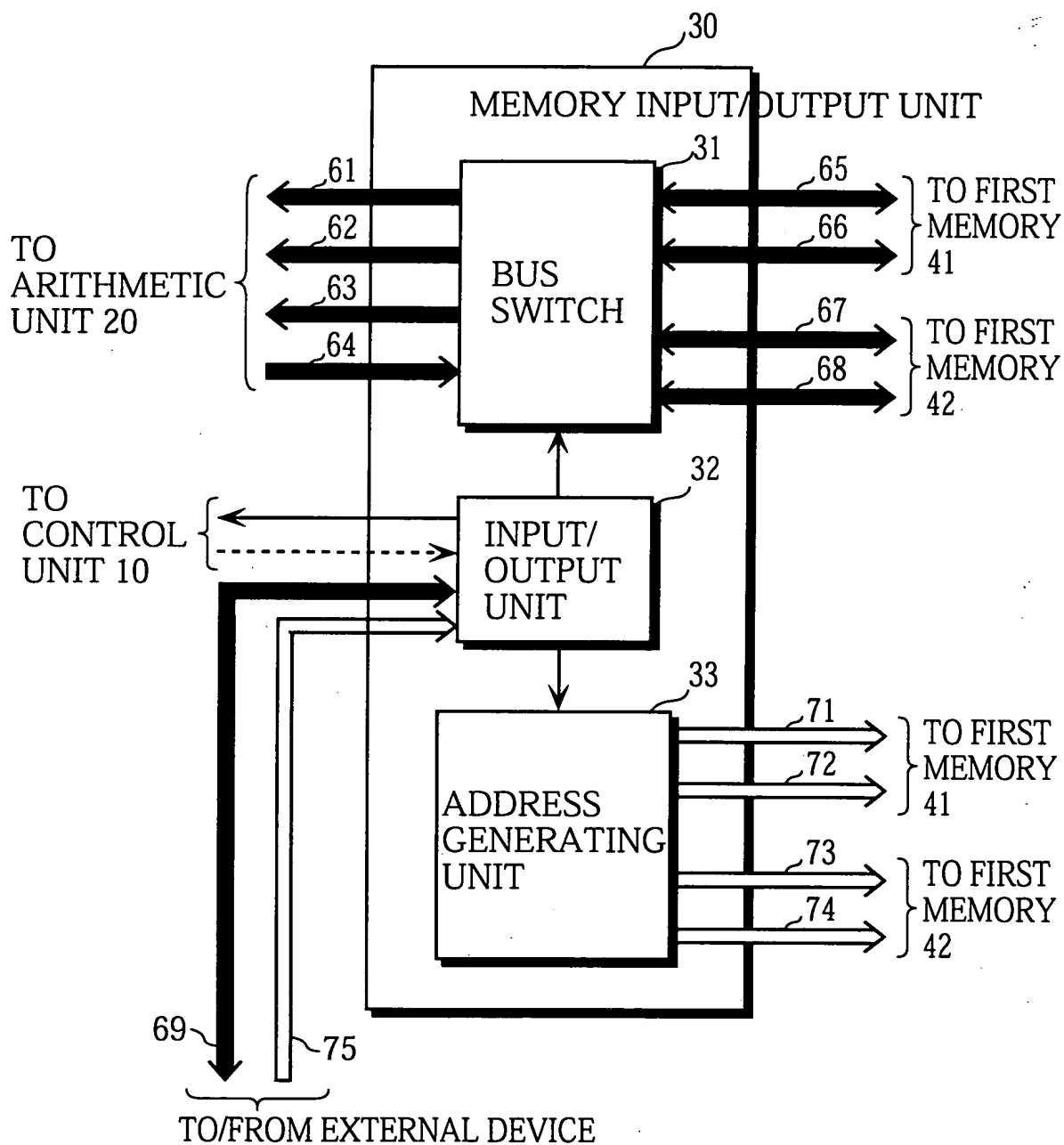


FIG. 4

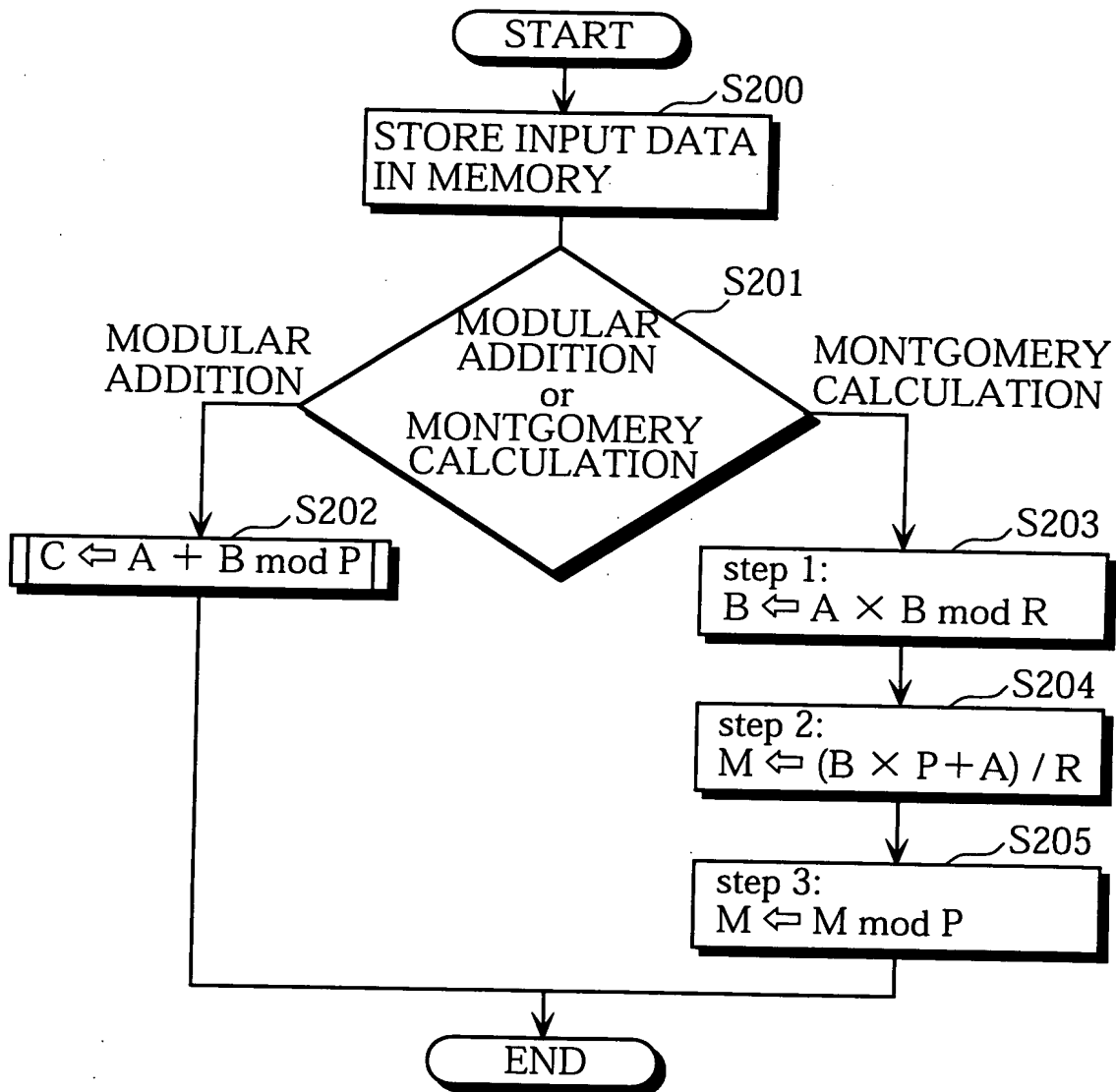


FIG. 5

CALCULATION FORMULA	C=A+B mod P
EXAMPLE INPUT	<div> <div> <div>←32 BITS→</div> <div> A : 1011 · 100110 · 001110 · 011010 · 100101 · 10 </div> <div> a4 a3 a2 a1 a0 </div> </div> <div> <div>←160 BITS→</div> <div> B : 0100 · 101001 · 011011 · 010010 · 111010 · 00 </div> <div> b4 b3 b2 b1 b0 </div> </div> <div> <div> P : 1101 · 000100 · 111010 · 111001 · 100001 · 01 </div> <div> p4 p3 p2 p1 p0 </div> </div> <div> <div> Q : 0010 · 111011 · 000101 · 000110 · 011110 · 11 </div> <div> q4 q3 q2 q1 q0 </div> <div> (-P) </div> </div> </div>

FIG. 6A

41

a0
a1
a2
a3
a4
.
.
p0
p1
p2
p3
p4
.
.
q0
q1
q2
q3
q4

FIG. 6B

42

b0
b1
b2
b3
b4
.
.
c0
c1
c2
c3
c4
.
.
w0
w1
w2
w3
w4

FIG. 7

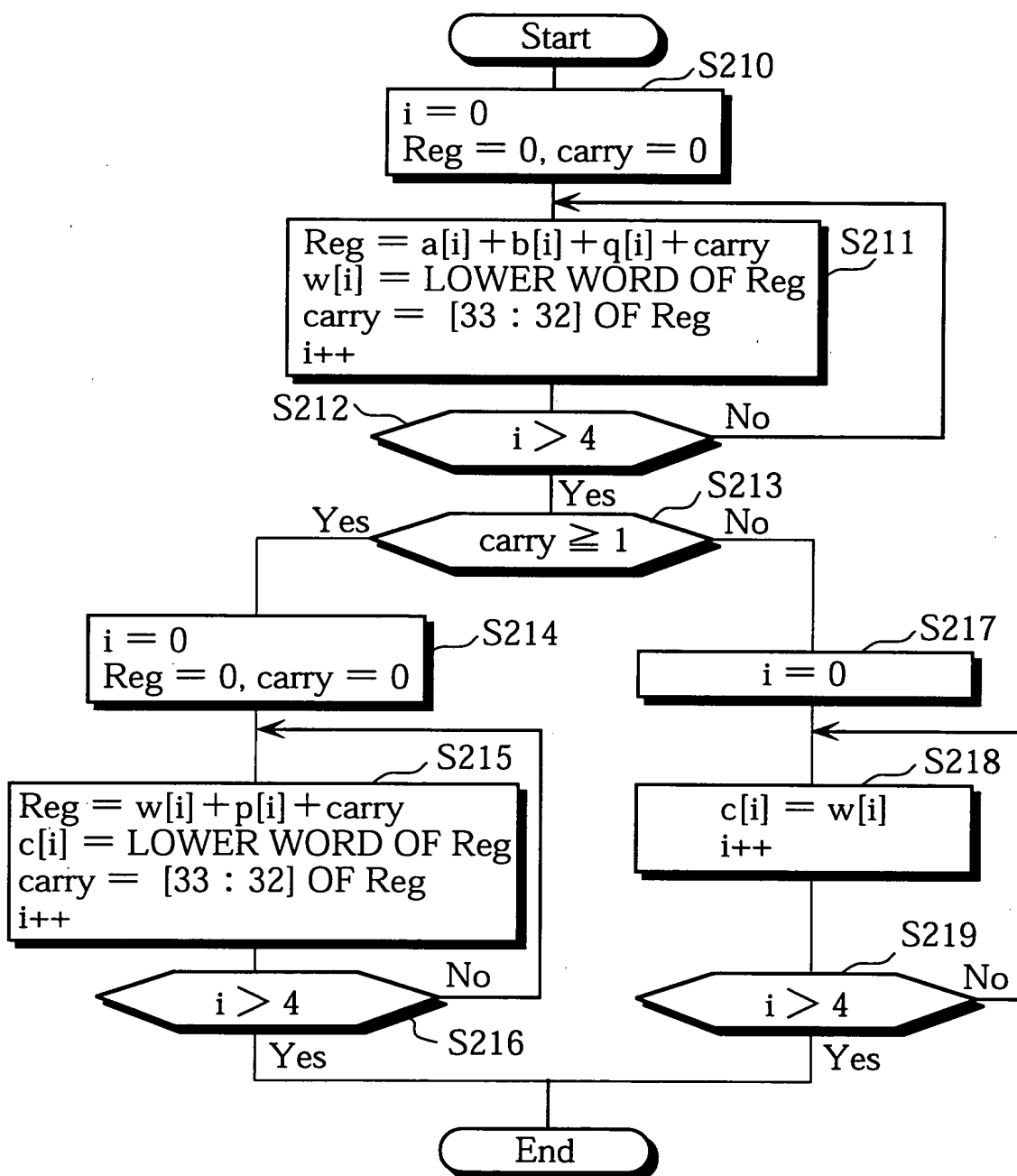


FIG. 8A

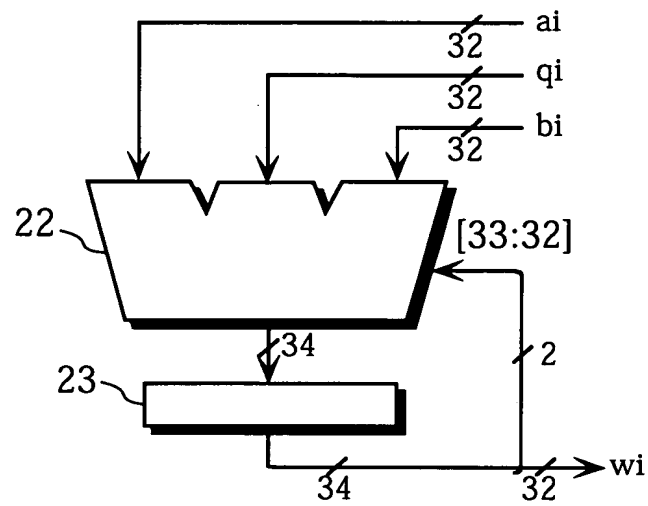


FIG. 8B

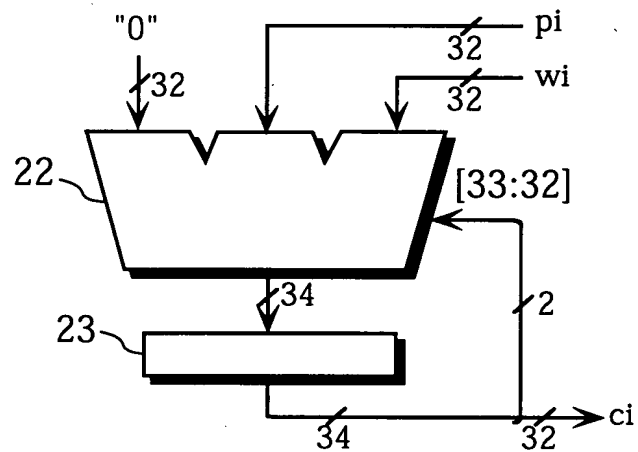
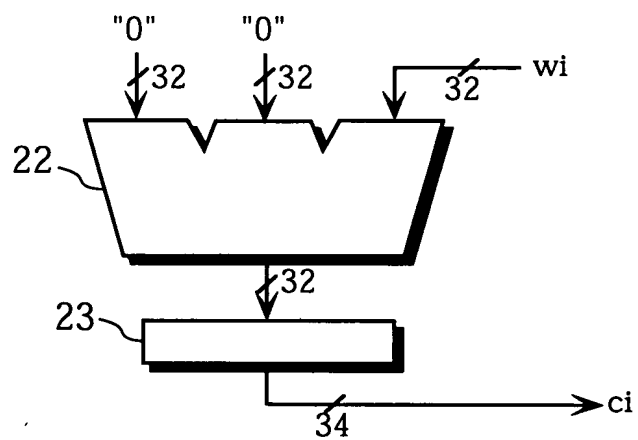


FIG. 8B



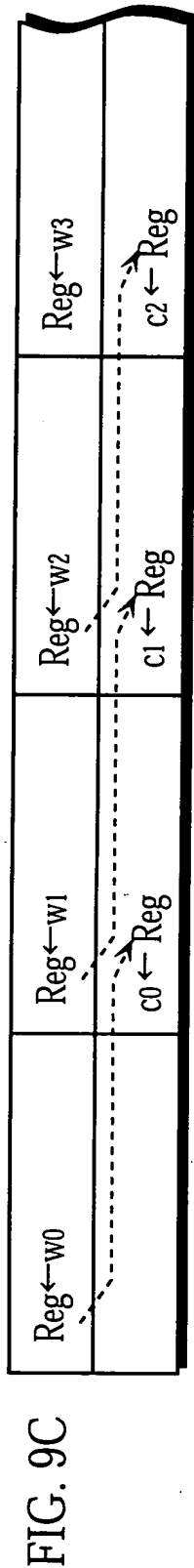
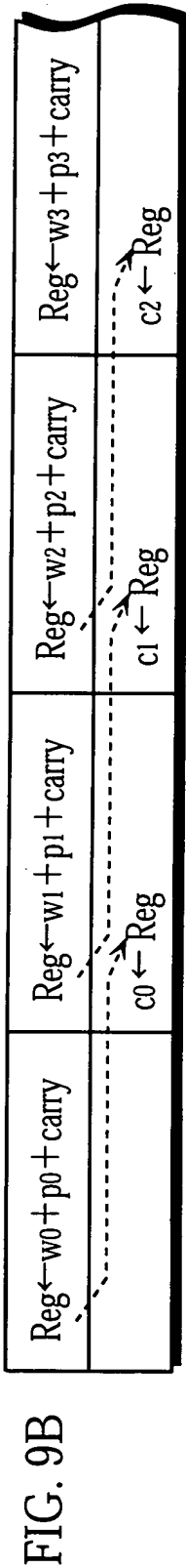
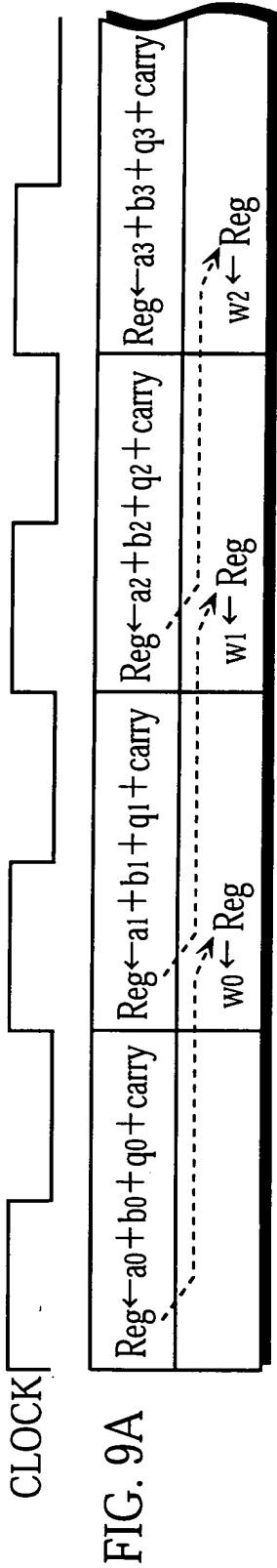


FIG. 10

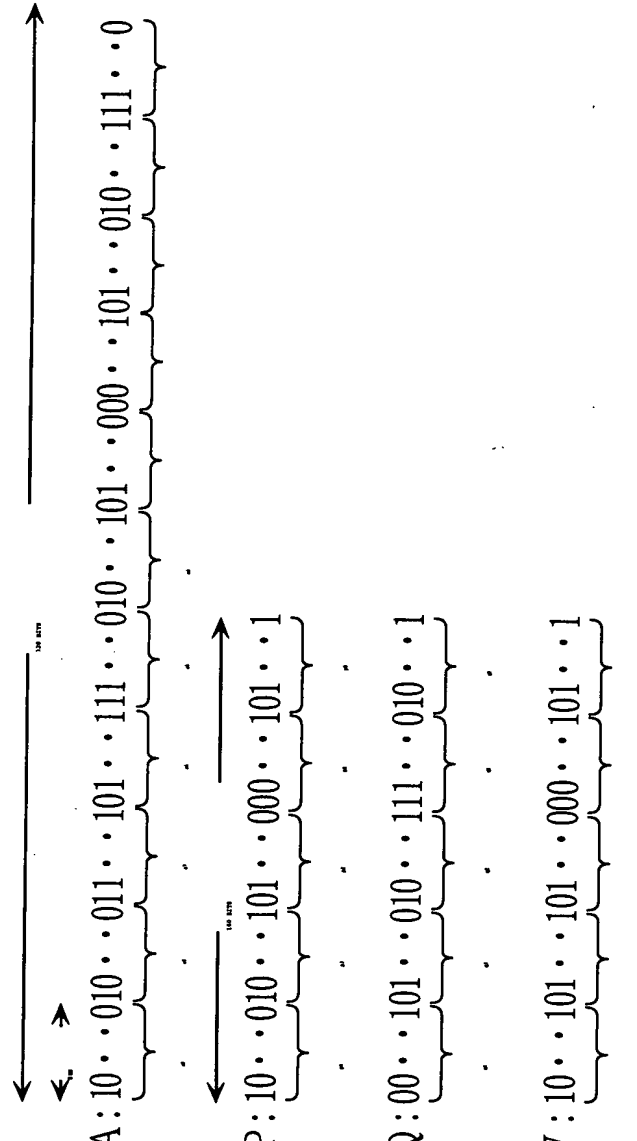
<p>CALCULATION: FORMULA</p>	<p>INPUT : A</p> <p>PRECOMPUTATION : $V = -P^{-1} \bmod R$ ($R = 2^{160}$)</p> <p>OUTPUT : $M = A \cdot R^{-1} \bmod P$</p> <p>PROCESSING : step 1 $B = A \times V \bmod R$</p> <p style="padding-left: 40px;">: step 2 $M = (B \times P + A)/R$</p> <p style="padding-left: 40px;">: step 3 OUTPUT $M \bmod P$</p>
<p>EXAMPLE INPUT</p>	 <p>A: 10 · 010 · 011 · 101 · 111 · 010 · 101 · 000 · 101 · 010 · 111 · 0</p> <p>P: 10 · 010 · 101 · 000 · 101 · 1</p> <p>Q: 00 · 101 · 010 · 111 · 010 · 1</p> <p>V: 10 · 101 · 101 · 000 · 101 · 1</p>

FIG. 11A

a0
a1
a2
a3
a4
a5
a6
a7
a8
a9
.
.
p0
p1
p2
p3
p4
.
.
q0
q1
q2
q3
q4
.
.
m0
m1
m2
m3
m4

FIG. 11B

v0
v1
v2
v3
v4
v5
.
.
b0
b1
b2
b3
b4
.
.
c0
c1
c2
c3
c4
c5
.
.
e0(0xffffffff)
.
.
m0
m1
m2
m3
m4

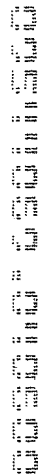
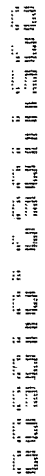
[illegible][illegible]

FIG. 13

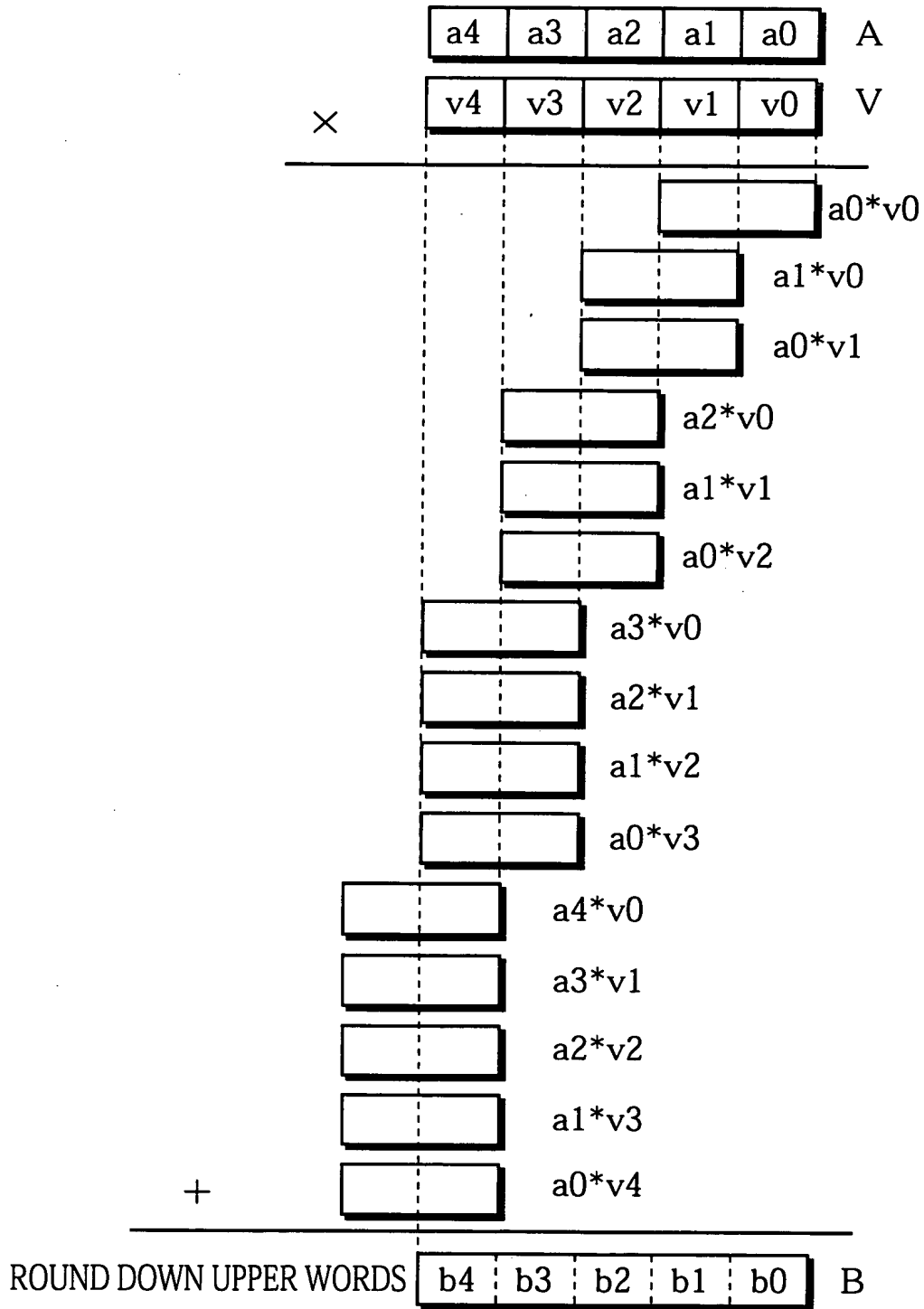


FIG. 14A

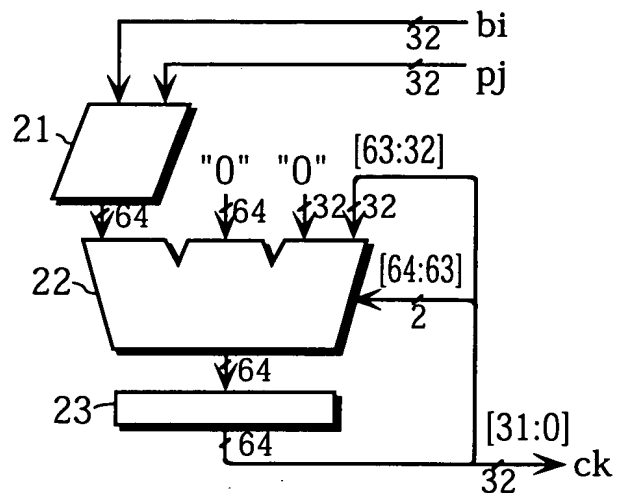


FIG. 14B

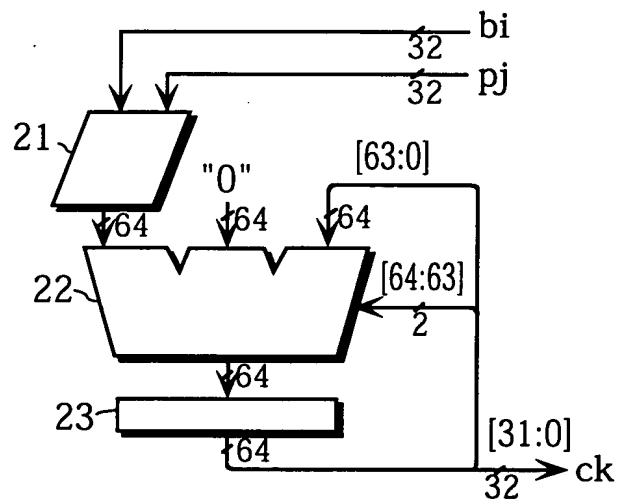


FIG. 14C

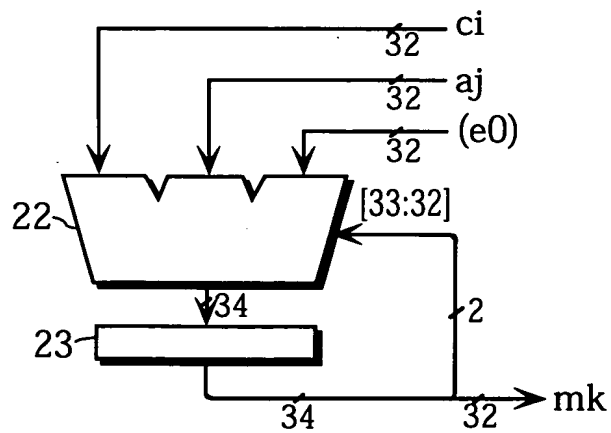


FIG. 15

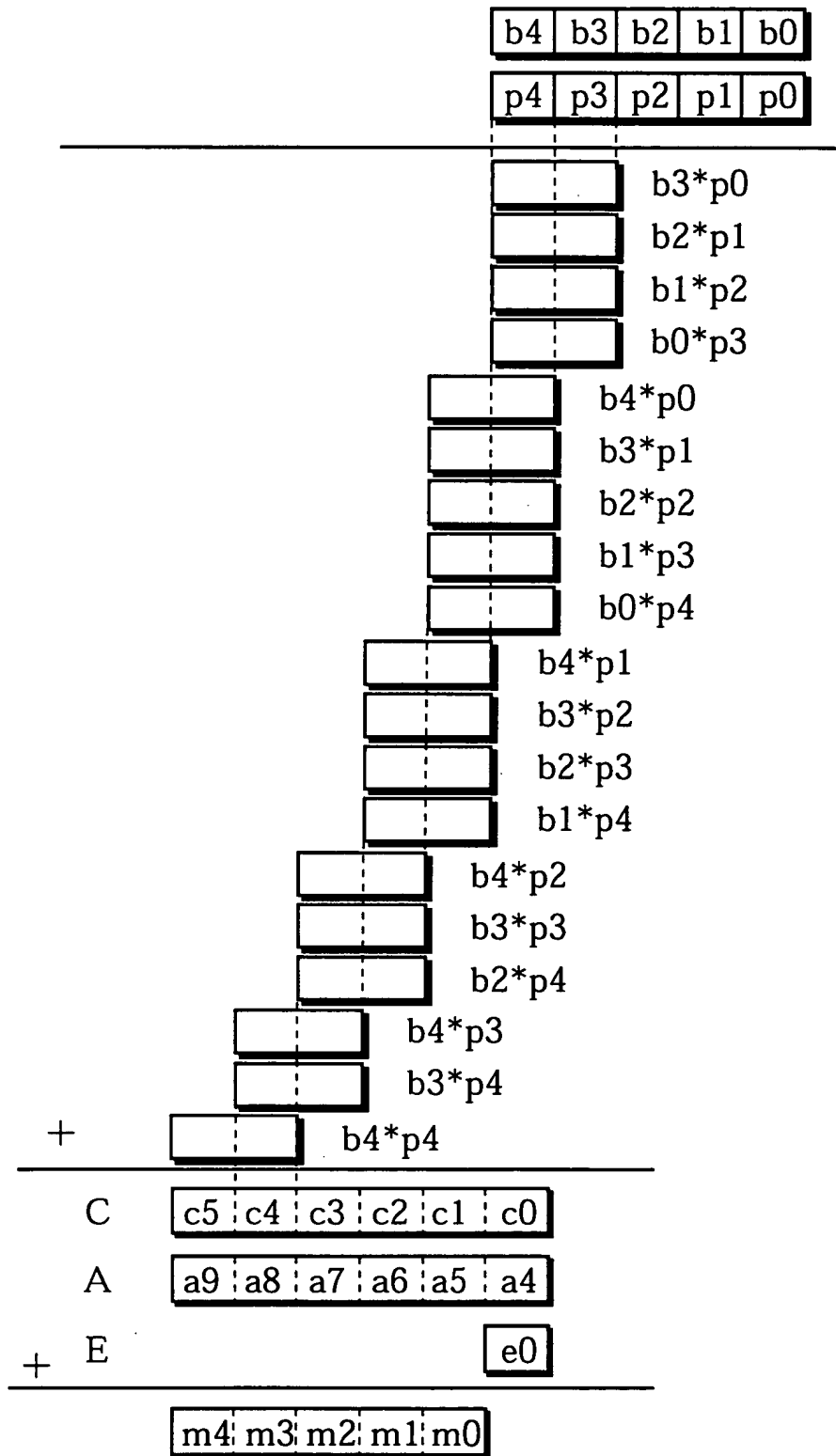


FIG. 16A

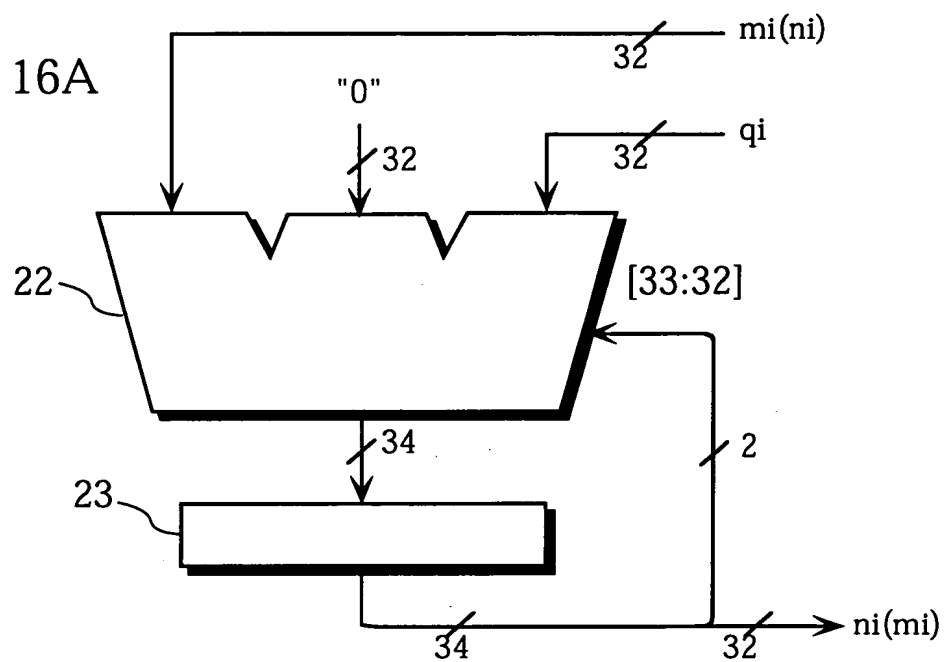


FIG. 16B

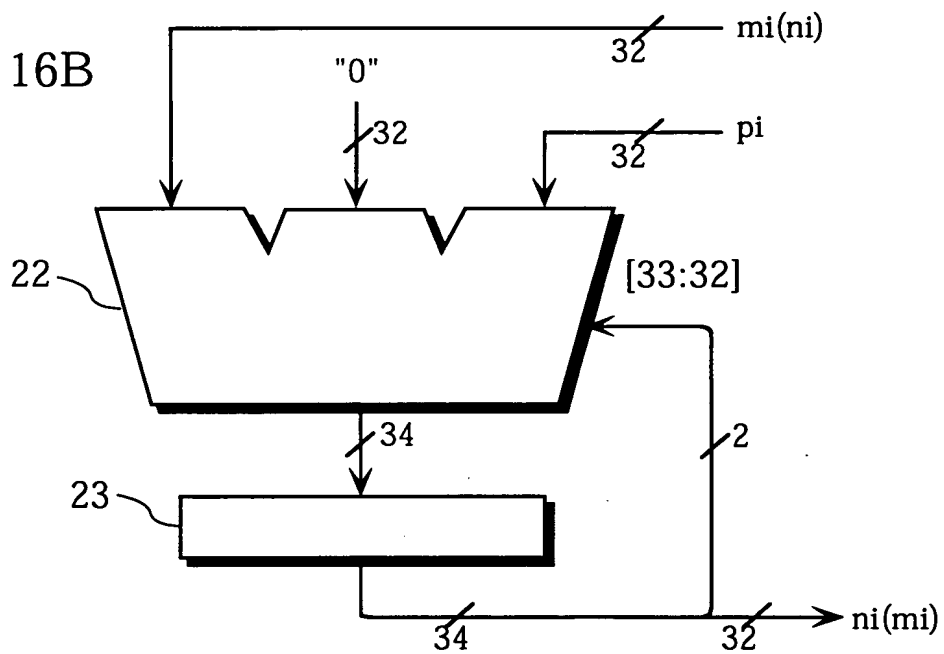


FIG. 17

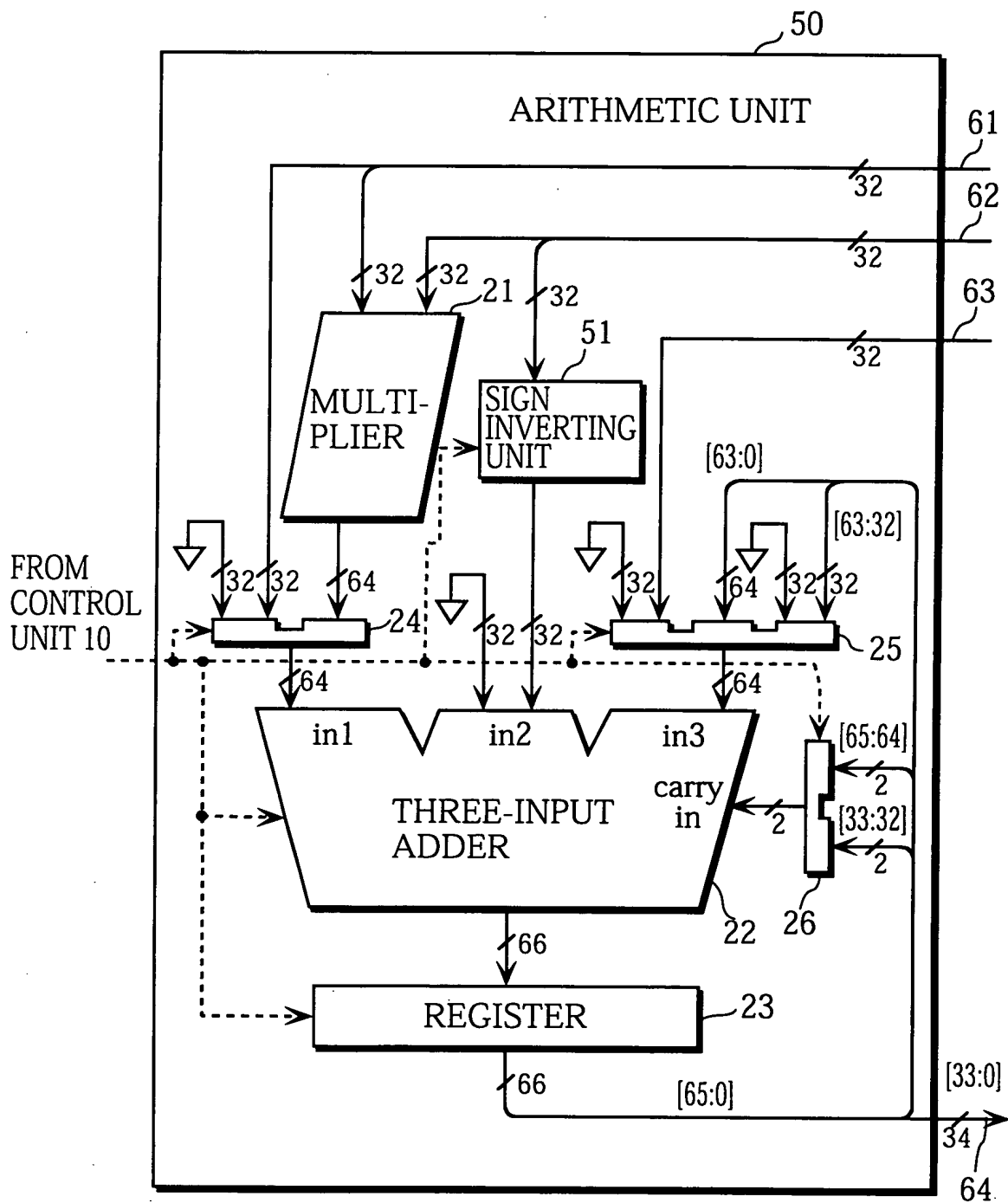


FIG. 18A

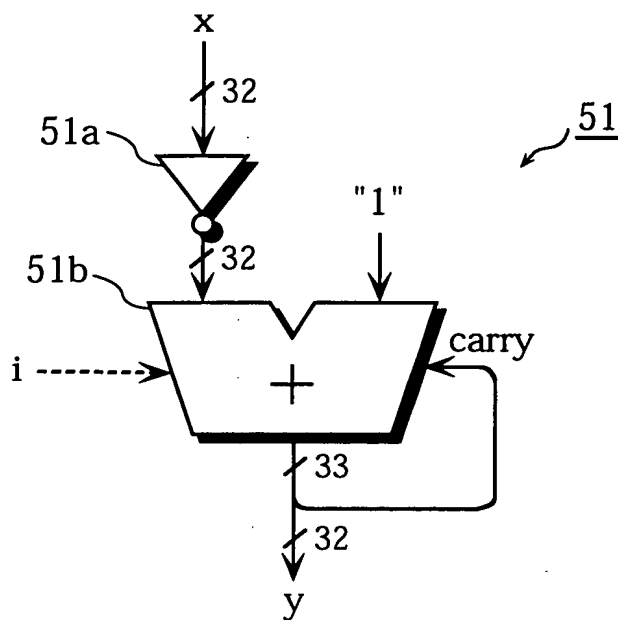


FIG. 18B

